Microsoft key messages for the hearing on "Cybercrime and Cyber Security" on 7 June 2017

The Initiative report of Civil Liberties Committee of the European Parliament on the "fight against cybercrime" is timely, considering cybercrime threats, the upcoming review of the European cybersecurity strategy, and the current work by the Commission and Council on improving cross-border access to electronic evidence

The draft report rightfully stresses the increase as well as changing nature of cybercrime, and the role that service providers, customers, and law enforcement play to improve prevention efforts.

Microsoft employs 3,500 security engineers, and works with the entire ecosystem to address security threats comprehensively. Nonetheless, as recent incidents demonstrate, nation-state action to stockpile vulnerabilities undermine prompt efforts to identify and patch them, and customer action is needed to maintain systems under their control. Information technology basics like keeping computers current and patched are a high responsibility for everyone.

Regarding cross-border law enforcement efforts to seize electronic evidence in criminal investigations, a more harmonized EU framework is needed to address the need for safeguards, certainty, and accountability – considering all relevant interests in public safety, data protection, sovereignty of nations, and trust in the digital economy.

The LIBE committee plays an important role to ensure any EU framework protects citizens' fundamental rights, and we have suggested a few amendments to the draft report to underscore the need to avoid disproportionate public authority interference with such rights.

We also emphasize the need for an e-evidence framework to require law enforcement demands for data be directed in the first instance to controllers or owners of data, and for such a framework to protect providers and other parties from demands that could create conflicting legal obligations

The draft report includes references to the important uses of encryption to protect data, and this needs to be emphasized. Everyone depends on encryption, including governments. A requirement to enable decryption of all services, as suggested in the draft report, does not take into account the differences in services. We would not apply directly the same safety regulations to planes as to trains, even though both provide transportation services. This topic requires a more nuanced consideration.